KETS Technical Standards Information Document

Wireless Local Area Network (WiFi)

Last Reviewed: 3/31/2015
Last Updated: 3/31/2015

Prepared by Paul Shoemaker

Department of Education
Office of Knowledge, Information and Data Services,
500 Mero Street
Frankfort, KY 40601
(502) 564-2020

Document Owner:	Paul Shoemaker	Date Created:	Aug. 16, 2006
Approver(s):	KIDS Leadership	Date Approved:	Feb. 28, 2008

Summary: The document establishes the standards required for the implementation of Wireless Local Area Networks (WLAN) within the Kentucky Education Technology Systems (KETS) statewide network. Technical implementation steps including security (network and physical), password configuration, encryption, SSID configuration and other implementation considerations are contained within this standard for guidance as local K12 districts implement this technology.

Purpose and Scope: Wireless networks must be carefully planned in order to provide a secure and reliable service to the end user. Although, this document is not intended to be a comprehensive guide to the implementation of wireless technology, it should be treated as a baseline for securing wireless networks.

Reason for Implementing: The Office of Knowledge, Information and Data Services (KIDS) is responsible for ensuring that the Kentucky Education Technology Systems (KETS) statewide network is secure and reliable. Over the past several years Wireless Local Area Network (WLAN) communication has become an increasingly popular means of connecting mobile devices such as laptops, PDAs and Smart Phones to the Internet and the Local Area Network. The number of planned and previously implemented Wireless LANs has increased to the point that standards and practices need to be articulated for this network service.

I. Wireless Local Area Networks (WLAN)

1. WLAN Acceptable Use

   A) Any user that requires access to wireless network services should be required to read and sign a copy of the district or school's Acceptable Use Policy prior to gaining access to the Wireless Network.

   B) Users should understand that wireless networks are inherently insecure. Therefore, the transmission of sensitive/confidential data should be encrypted at the application layer (i.e. SSL, SSH) or should not be allowed to be accessed via wireless network.

2. Installation and Security

   A) Access Control (MAC address filtering) / 802.1x Authentication – (Pending future KETS Enterprise design implementation)

1) Although, it is highly recommended that 802.1x authentication be implemented in conjunction with Media Access Control (MAC) address lists, it is not a requirement at this time. For small wireless network installations (e.g. <30 devices) Media Access Control (MAC) address lists may be used in place of 802.1x Authentication. For larger wireless network installations (e.g. >30 devices) 802.1x Authentication must be implemented. In either small or large deployments, if 802.1x Authentication is implemented, Media Access Control (MAC) address lists are not required.

B) Configuration Passwords

1) All Wireless Access Point (WAP) management interface passwords must be changed from the default. Passwords must be difficult to guess and at a minimum be alphanumeric 8 or more digits in length. See the SANS Institute’s Password Policy for more information on creating secure passwords.

2) All Wireless Access Point (WAP) management interface passwords should be changed periodically to reduce security threats.

C) Connectivity

1) Ethernet hubs transmit data to every device on the network segment, including wireless devices. An intruder would not only be able to see the data transmitted via the wireless network, but all devices connected to the segment including hard wired LAN devices. Therefore, all Wireless Access Points (WAP) must be connected directly to an Ethernet switch.

D) Dynamic Host Configuration Protocol (DHCP)

1) Some Wireless Access Points (WAP) can be configured to give out Dynamic Host Configuration Protocol (DHCP) addresses directly. All Wireless Access Points must not be configured to assign DHCP addresses. Instead, they should be configured as a pass-thru or bridge device and allow Active Directory to assign and manage all DHCP address assignments.

E) Network Address Translation (NAT)

1) Network Address Translation (NAT) allows several wireless devices to share a single IP address on the Local Area Network. This feature must be disabled on all Wireless Access Points because any accountability for those wireless devices would be lost.

F) Encryption

1) All Wireless Access Points (WAP) must be configured with the highest possible encryption available. 128-bit Wi-Fi Protected Access (WPA) is preferred. However, some legacy devices do not support WPA, therefore it is not required. In such cases 128-bit Wired Equivalent Privacy (WEP) must be used.

2) All Wireless Access Point (WAP) keys must be changed on a periodic basis.

G) Physical Security and Placement

1) Wireless Access Points (WAP) should not be placed in locations that make them easy for someone to steal. All Wireless Access Points (WAP) should be either placed in a locked wiring closet, placed in a lockable enclosure, hidden from site above ceiling tiles or secured in such a way that removing them would damage them.

2) A vendor site survey is not required prior to the implementation of a Wireless Local Area Network (WLAN), however it is recommended. As the placement of the Wireless Access Point (WAP) must be carefully planned and should take the following into consideration:

a) If Wireless Access Points (WAP) that are on the same RF channel are placed too close to one another, the overlap may result in interference in the overlapped area.

b) Wireless Access Points (WAP) should be strategically located to prevent the interception of wireless signals by unauthorized individuals. The range must be tested to ensure that signals are not being transmitted outside the intended coverage area.

c) Wireless Access Points (WAP) must be installed so they do not violate state or local fire codes.

d) The number of devices a Wireless Access Point (WAP) can support can differ depending on the type of use that is expected. The following should be used as an initial starting point for determining the number of Wireless Access Points (WAP) required to provide Wireless Local Area Network (WLAN) coverage.

- Heavy Usage – (up to 20) devices all accessing the network concurrently to access web pages, low to medium quality streaming video, large file transfers, etc..
- Medium Usage – (21 to 40) devices using the network, but not in a coordinated fashion. For example all working independently on projects, etc.
- Light Usage – (41 to 60) devices using the network on a casual basis and concurrency of use is random and minimal. This would also include large numbers on concurrent users accessing low bandwidth applications such as email.

H) Security Review

1) Periodic security reviews should be performed to ensure that changes to the Wireless Local Area Network (WLAN) have not exposed the network to intruders.

2) The network should be periodically scanned to detect unauthorized wireless devices.

I) Security Switch

1) Wireless Security Switches are not required as long as all security measures outlined in this document are met. However, wireless security switches are highly encouraged in large deployments due to the many benefits that they provide including: Centralized Management for up to 120 Wireless Access Points, Acceptable User Policy Enforcement, Quality of Service (QoS) Policy Enforcement, Usage Tracking, Location Tracking, etc…

J) Service Set Identifier (SSID)

1) The Service Set Identifier (SSID) should not openly identify the Local Area Network (LAN) or its purpose and should be constructed as securely as a password.

2) The regular broadcasting of the Service Set Identifier (SSID) must be disabled on all Wireless Access Points (WAP).

K) Simple Network Management Protocol (SNMP)

1) Simple Network Management Protocol (SNMP) settings should be changed from the default and should have access control lists where possible.

L) Updates (Firmware & Software)

1) Software and Firmware updates from the wireless manufacture(s) should be applied to Wireless Access Points (WAP) and wireless devices as soon as possible after release to correct any security vulnerabilities.

M) Virtual Private Network (VPN) Integration

1) Virtual Private Network (VPN) Integration is currently not required in Wireless Local Area Network (WLAN) deployments. However, VPN solution can be utilized to provide an extra layer of protection between the WLAN and the LAN.

N) Wireless Local Area Network (WLAN) Technology

1) All Wireless Access Points (WAP) must support 802.11 a/b/g standards and n once standard has been adopted.

Acronyms/Abbreviations:

- DHCP - Dynamic Host Configuration Protocol
- MAC Address - Media Access Control Address
- NAT – Network Address Translation
- SNMP – Simple Network Management Protocol
- SSID – Service Set Identifier
- VPN – Virtual Private Network
- WAP – Wireless LAN Access Point
- WEP – Wired Equivalency Privacy
- WLAN – Wireless Local Area Network
- WPA – Wi-Fi Protected Access

Approved Product

Manufacturer	Contract Holder/ Sales Agent	KETS Master Agreement/ Contract Number
Enterasys Network Inc.	Enterasys/ Dell Computer Corp.	MA-758-C04019663
Nortel	IBM Corporation	MA-758-C03377448
Nortel	Pomeroy IT Solutions	MA-758-C03377493

Quality Records

Title	Location Kept	Duration Kept	Disposal Method

Standard Expectations

System Status	Expectation	Action
Existing	Existing System Grandfathered	No action required until system upgraded or replaced.
System Upgrades	Upgrades to system should be in compliance with standards	Move system towards compliance.
New Systems	Meet or exceed standards as stated.	Meet or exceed standards as stated.